18 January 2021

Jenny Lyons
Senior Specialist — Credit, Retail Banking and Payments
Financial Services Group
Australian Securities and Investments Commission
Level 7, 120 Collins Street, Melbourne, 3000
Jennifer.Lyons@asic.gov.au

Dear Jenny

ASIC's ePayments Code review

Thank you for the opportunity to comment on ASIC's potential changes to the ePayments Code. The Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia wish to address one aspect of the proposals in this letter: screen scraping and pass code security requirements. We understand that the Consumers Federation of Australia will be commenting on other aspects of the proposals in a separate submission.

In short, we recommend that ASIC reconsider its current position with respect to screen scraping and pass code security requirements as expressed in the December 2020 proposals.

ASIC's proposed approach to screen scraping and pass code security requirements

We note in the letter dated 9 December that ASIC propose the following approach to screen scraping and pass code security requirements:

> *5.2 Neither prohibit nor expressly permit what is often referred to as 'screen scraping' or other sharing of customer data with third parties.*

This is an illogical position – it is a decision to "do nothing". Doing nothing is a choice. That choice is one that in effect turns a blind eye to the practice of screen scraping, thereby permitting and condoning it.

This is also an untenable position. ASIC is aware that screen scraping is an inherently unsafe online practice. The position ASIC is therefore taking directly contradicts not just government[1] and industry advice but ASIC's *own* advice to consumers.

ASIC's Money Smart website tells people that that:

> *"Don't tell anyone your passwords - a legitimate business or company should never ask you for your password."*[2]

Yet inexplicably ASIC says it will not take a "position" on whether screen scraping should be permitted under the ePayments Code, a process which can only be facilitated by the provision of a password.

To be clear, it is a fundamentally dangerous practice to hand over one's banking password details because such a practice makes passwords and security information more vulnerable to breach and can lead to people being scammed, people having their identities or money stolen, errors to occur in responsible lending checks or worse.

For ASIC to elide this principle in the key document that regulates this area is unsupportable.

Effective messaging, the E-payments Code and the Consumer Data Right

We note that ASIC propose to:

> *5.7. Engage with digital data capture service providers, with the aim of developing consistent, useful and effective messaging for consumers, to enable the consumer to make informed decisions about using the service.*

Relying on disclosure in the screen scraping context runs counter to ASIC's acknowledgement that reliance on disclosure as a regulatory tool more generally is ineffective as set out in Report 632.[3] That report was a seminal contribution to our understanding of disclosure as a regulatory tool and the research findings set out in that report should be used to guide the way ASIC turns to disclosure, compared to other regulatory options.

ASIC should understand that financially vulnerable people desperate to access credit via a service that uses screen scraping technology will not concern themselves with the nuances of privacy protections or any messaging produced by businesses to allow consumers "to make informed decisions about using the service." If obtaining credit means engaging with unsafe digital capture practices financially vulnerable people will do so and end up with lower privacy protections than customers seeking loans from CDR accredited lenders.

---

[1] The Australian Government's StaySmartOnline website states: "Keep your passwords secure by taking measures to protect them: Don't share your passwords with anyone. https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/passwords-business

[2] https://www.moneysmart.gov.au/scams/avoiding-scams

[3] ASIC REP 632 Disclosure: Why it shouldn't be the default, October 2019 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/

Personal responsibility is commonly brought up as an argument to maintain the ability for consumers to choose to use services that use screen scraping technologies. But when consumers are excluded from accessing mainstream credit and these provider will only use screen scraping technology – there is no true choice here for a consumer to decide between obtaining credit and giving up privacy and other rights. Genuine consent is absent where the power is held by the provider.

Even non-financially vulnerable consumers may hold misplaced trust in a financial advisor or accountant who uses screen-scraping technologies. Indeed there is significant research that trust increases when a financial advisor provides information on conflicts of interest because the consumer believes they are being transparent and is therefore more deserving of trust.[4] The same principle applies here where messaging has the potential to reassure a consumer to use an unsafe pass code service rather than deciding against it.

Rather than relying on disclosure and placing the responsibility all on the consumer to be informed, obligations needs to be put in place to ensure that consumer protections are built in to the very design of data collection and handing processes. Businesses should be required to adhere to using the principles of privacy by design and security by design.

More importantly ASIC needs to take a stronger approach to regulating this space by requiring that businesses adhere to safe practices.

The Consumer Data Right has now been established to facilitate Open Banking and should be a key consideration in ASIC's deliberations with respect to updating the ePayments Code.

The Consumer Data Right was established to provide a fast, safe, and secure process to access personal and financial data. The Consumer Data Right is fundamentally a right to port and transfer one's own personal financial data – similar to screen scraping – but in a safe environment "ensuring …high levels of privacy protection and information security for customer data"[5]

The approach that ASIC should take here is therefore to require that digital data capture can only take place within the framework of the Consumer Data Right and that all businesses looking to "screen scrape" should be accredited under the Consumer Data Right regime.

This would provide a key incentive to take up the CDR and Open Banking as well and support the government's aim to promote the CDR.

---

[4] James Lacko and Janis Pappalardo, *The effect of mortgage broker compensation disclosures on consumers and competition: A controlled experiment*, *Federal Trade Commission Bureau of Economics Staff Report*, 2008 referenced in Financial Services Authority, Financial Capability: A Behavioural Economics Perspective, 2008*: "Even if the disclosure is noticed by consumers, it may have the effect of increasing trust in advisers rather than making consumers more wary."*

[5] The Hon. Scott Morrison, Treasurer, Media Release *More power in the hands of consumers*, 21 September 2018, http://sjm.ministers.treasury.gov.au/media-release/087-2018/

Vulnerable consumers

We note that ASIC propose the following.

> *5.3. Bearing consumer vulnerabilities in mind, do not qualify the PSRs by adding to the exceptional situations in which disclosure of a pass code is permitted. Instead, include a clause in the Code that states in general terms that vulnerability should be considered by the subscriber when applying the unauthorised transaction provisions.*

Stating that vulnerability should be considered by the subscriber is weak and will allow a subscriber to consider vulnerability and discount it at any point for any reason. Under this proposal, there will be no requirement to act when vulnerability has played a central role in the obtaining of a pass code.

This could be easily avoided by simply not allowing any business to obtain a pass code, and requiring subscribers to be accredited under the consumer data right regime.

Screen scraping is unsafe, unstable and prone to errors

Finally, we believe it is important to share recent case studies obtained by our organisations to demonstrate the harm in the approach currently being taken by ASIC under the ePayments Code as well as demonstrate how the approach being proposed will not address the harms.

As ASIC is more than aware, it is a dangerous practice to hand over one's password details because encouraging such a practice makes passwords and security information more vulnerable to breach and can lead to people being scammed, people having their identities or money stolen or worse.

Case study Edward's story - C197644

Edward was searching for good rate deals for credit on the internet. Edward found a rate on a lender's website and he then contacted them for further information. The lender then sent him an email. Edward responded and provided information to begin a process he believed would lead to him being provided with an offer. As a part of this process Edward was required to provide his details to his bank account and to obtain his credit report in order for him obtain his "tailored interest rate."

Before he knew it Edward had been approved for a $15,000 loan with the money deposited into his account. Edward had only been shopping around and had not expected to be provided with the money - merely an offer. The lender refused to rescind the contract until they had been told that he had contacted Financial Rights. In the meantime Edward had in fact found a better deal and wanted to go with this other lender.

Source: Financial Rights Legal Centre

Screen scraping is fundamentally unstable and the technology breaks down regularly. Screen scraping scans the existing consumer-facing web portals of financial providers, which means

that if there is a small change to a website it can create stability issues for those screen scraping tools. Open banking APIs under the CDR do not have this issue.

Case study 's story – Sally's story - C208390

In 2019, Sally formed an online romance which turned out to be a romance scam. The scammer manipulated Sally into applying for loans to pay money to him. Sally was not initially able to procure any loans because of her financial circumstances. Sally was surviving on Newstart benefits and casual work and renting a NSW Housing Commission rental property with her dog. Sally also had a number of medical conditions treated by medication.

Sally provided the lender with access to her bank statement using Illion software to assess her income against her essential living expenses. The lender approved the loan and the funds were transferred.

The scammer told Sally to transfer the loan payment to him through a series of transactions and she did so under the promise he would travel to Australia to be with her. The scammer never came to Australia and Sally realised she was scammed. Sally lodged a complaint with the online dating site and ScamWatch.

Sally was able to keep up with the loans only after borrowing money from family and friends but ultimately she could not keep up with the payments.

The lender did not agree to a full debt waiver on compassionate grounds as they believed Sally could still afford the repayments if further options were explored and offered a three-month moratorium with nominal payments. Sally's financial circumstances did not change with no prospect of her being able to make payments because of her age and ailing health conditions.

In examining the responsible lending check undertaken – obtained via screen scraping by Illion the algorithm identified certain monthly income and expenses. However, the Illion algorithm did not pick up other obvious monthly living expenses in their assessment. With this corrected, Sally's total net income would have been $25 per month. This would not be enough to afford the monthly loan repayments of $280 required.

The overreliance on the flawed screen scraping process and not questioning Sally about the nature of her expenses resulted in a failure to ascertain all of her living expenses.

Source: Financial Rights Legal Centre

Case study Annabel's story - C196186

About 2 years ago, Annabel obtained a loan from a payday lender for $1,500. The lender uses a data aggregator with screen scraping technology to obtain required information for responsible lending checks.

In the 90 days before this loan was obtained, Annabel had entered into 2 other Small Amount Credit Contracts (**SACC's**) with the payday lender and was a debtor on 6 SACC's in total. This fact was noted in the loan application.

Annabel borrowed a further $700 in 2018.

Last September, Annabel's Centrelink benefit changed from DSP to Newstart, and Annabel was unable to afford repayments at the fortnightly rate of approximately $150.

In examining Annabel's situation, Financial Rights obtained documentation from the payday lender which was based on the use of a data aggregator's screen scraping tool.

The report was riddled with inaccuracies including:

- Incorrect calculations with respect to her net monthly income which inappropriately took into account lump sum cash advance payments she received from Centrelink and assumed they were additional regular income.
- Missing information with respect to EFTPOS payments.

Source: Financial Rights Legal Centre

Case study Gavin's story - C196186

Gavin has payday loans totaling $4,000. In December last year he applied for loans with a payday lender where he was declined on two applications but accepted into two other loans.

Gavin has struggled to pay the loans as he has Child Support of $400 per fortnight and rent. Gavin pays $400 a fortnight to the payday lender with fees of $80 for each loan per fortnight.

Financial Rights has in representing Gavin discovered when looking at the data aggregation provided for responsible lending purposes, it was riddled with errors – including categorizing his café payments for coffee as rent.

Source: Financial Rights Legal Centre

Case study Jane and Bernie's story

Jane and Bernie (names changed) were a couple with 4 dependent children. Their income derived from Centrelink and Bernie's casual job.

In late 2016 Bernie decided to purchase a car and was referred to a broker. The broker failed to properly explain the agreement they were jointly entering (even though the car was for Bernie) and Jane did not understand the relationship between the broker and the lender.

While the finance company appears to have roughly assessed Jane and Bernie's incomes correctly, it appears to have used only a one-page account scraping document pertaining to an account in Bernie's sole name, which was submitted in the loan application, to verify expenses. The finance company does not appear to have obtained copies of bank statements for Jane and Bernie's joint accounts or Jane's sole accounts at the time, which would have shown whether the loan was unaffordable for Jane and Bernie.

Both the broker's loan application and finance company's assessment appear to significantly understate Jane and Bernie's living expenses, with the expenses listed on the lending assessment document totalling even less than that on the loan application. The finance company appears to have applied an arbitrary benchmark that was lower than both the Henderson Poverty Index (HPI) and Household Expenditure Measure (HEM) benchmarks for that quarter.

They soon fell into arrears on the loan as the loan was not affordable for Jane and has caused her substantial hardship.

Source: Consumer Action Law Centre

In addition to customers being asked to provide access to online banking details so a third party can access their account for loan assessment purposes – we have begun to see example of this practice occurring at the time they are seeking a variation on the grounds of hardship. This is a point in time when people are prone to targeted pay day lending offers.

Case study Zed's story

Zed (name changed) was trying to negotiate a hardship variation with Zip Money. Zip Money were aware that Zed had physical issues, an acquired brain injury and was taking medication that affected his cognitive ability. They also knew that a financial counsellor was assisting him. Despite this, Zip Money contacted Zed directly stating that in order to assess his variation they would need copies of his bank statements. Zip Money stated that to make this "easier" he could supply his banking credentials to the third party company

Credit Sense. Concerned about what to do, Zed got in touch with his financial counsellor for advice.

Source: Consumer Action Law Centre

Usually people have no choice but to hand over their password details – which includes agreeing to a range of uses of the information gathered including third party marketing – something that is not allowed under the upcoming CDR.

For example, Illion states that it may:

> ***Illion's Privacy Policy***
>
> *Illion's privacy policy includes the following terms for use of personal information:*
>
> - *to include in one or more of our databases so that we can provide it to our customers as part of the product or service they select;*
> - *sharing with our group companies to assist with the management of information or delivery of our services;*
> - *sharing with our group companies, affiliates and partners who will collect, hold, use and disclose Personal Information shared with them by us to create and sell risk analysis and other information products; and*
> - **to assist our customers to identify products and services and special offers that might be of interest to individuals and businesses (limited to Marketing Services only**).[6]

We are also aware of one pay day lender refusing to hand over the details of bank data that was used in a credit assessment and verification on the basis that that data is sourced:

> *from a third party … and they contain valuable intellectual property in relation to income and expense categorisation.*

And of course – other terms and conditions allow ongoing access to bank account information:

Prospa's consent to collect personal information states:

> *Bank Statements and third party account aggregation service provider: By obtaining from you access to your internet banking, our third party service provider will access your personal information for the purpose of providing your bank account information to us. We will obtain up to the last twelve (12) months bank transactions on the date you apply for a loan, in addition to further ongoing bank transactions for the term of the loan, for the purpose of assessing any future loan application or making any future offer to you.* **We note that your bank's terms**

[6] https://www.illion.com.au/privacy-policy-risk-marketing-solutions/

may prohibit you from sharing your login, so you agree to appoint our third party service provider as your agent to access your internet banking on your behalf solely for this purposes and you consent to our ongoing access to this information for the term of the loan and the purposes outlined above.[7]

We are aware of financially vulnerable clients providing log-in details to payday lenders, only to have the payday lender use the log-in details later to identify when a consumer is getting low on cash and subsequently directly advertise to that consumer. This has the effect of exacerbating financial hardship.

We would also note that there is a significant number of new avoidant credit options being introduced including BeforePay (with more than 100,000 registered users[8]), MyPayNow, AdvancePay that are all using screen scraping technologies.

Given the above – we strongly recommend that ASIC reconsider its current position as expressed in the December 2020 proposals.

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Drew MacRae, Policy and Advocacy Officer, Financial Rights on (02) 8204 1386.

Kind Regards,

Alexandra Kelly
Director of Casework
Financial Rights Legal Centre

Katherine Temple
Director Policy & Campaigns
Consumer action Law Centre

Fiona Guthrie
Chief Executive Officer
Financial Counselling Australia

[7] https://www.prospa.com/consent-information

[8] https://www.smartcompany.com.au/startupsmart/news/beforepay-fintech-wages-in-advance/